

IN THE SPECIFICATION:

Please amend the title as follows:

- - NON MALLEABLE ENCRYPTION AND SIGNATURE METHOD AND APPARATUS - -

IN THE CLAIMS:

1. (currently amended) A method comprising the steps of:

encrypting a data message m using a primary transmitter secret key z to form a quantity

E;

preparing a quadruplet (a_{new} , b_{new} , s_{new} , E) where:

$$a_{new} = z * y^c \text{ modulo } p;$$

$$b_{new} = g^c \text{ modulo } p;$$

$$s_{new} = \text{signature}_c(a_{new}, b_{new}, E);$$

where $y = g^x \text{ modulo } p$, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c

that was used to determine a_{new} and b_{new} .

verifying the signature s_{new} ;

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m.

2. (original) The method of claim 1 and wherein: